AMENDMENTS TO THE CLAIMS

Cancel Claims 9-11 and 29-31 without prejudice. Please accept amended Claims 1, 21, and 36 as follows:

Listing of claims:

1. (Currently Amended) A method for processing data, comprising the steps of:

obtaining a patient data record of a patient which includes patient identifying information;

removing the patient identifying information from the patient data record to generate a de-identified data record comprising unencrypted patient data in the patient data record which does not identify the patient;

generating an encrypted ID for the patient, wherein the encrypted ID comprises an encrypted representation of one or more items of patient identifying information; and

storing the encrypted ID with or in the de-identified data record,

wherein the step of removing the patient identifying information in the patient data record includes automatically removing patient identifying information from an unstructured data record by locating a text string in the unstructured data records that includes patient identifying information, and removing the text string from the unstructured data record, wherein the text string to be removed from the unstructured data record is determined based on a matching text string that is included in a database element of a structured data record associated with the unstructured data record.

2. (Original) The method of claim 1, wherein the step of generating an encrypted ID for the patient comprises encrypting the one or more items of patient identifying information using a public key.

3. (Original) The method of claim 1, further comprising securely maintaining a decryption key, which can be accessed by an authorized entity to decrypt the encrypted ID in the de-identified data record to re-identify the patient.

4. (Original) The method of claim 3, wherein the decryption key is a private key that is associated with the public key for encryption.

5. (Original) The method of claim 3, wherein the decryption key is a master private key that can decrypt de-identified data produced from many encryption/decryption key pairs.

6. (Original) The method of claim 1, wherein the step of removing the patient identifying information in the patient data record to generate a de-identified data record is performed in compliance with a Safe Harbor rule or Limited Data set Rule of HIPAA.

7. (Original) The method of claim 1, wherein the step of removing the patient identifying information in the patient data record includes automatically removing patient identifying information from a structured data record.

8. (Previously Presented) The method of claim 6, wherein the step of removing the patient identifying information from the patient data record comprises removing database elements that contain the patient identifying information.

9-11. (Canceled)

12. (Previously Presented) The method of claim 1, wherein the step of removing the patient identifying information from the patient data record includes automatically removing patient identifying information from an image.

13. (Original) The method of claim 12, wherein the step of automatically removing patient identifying information from an image comprises removing patient identifying information contained in structured fields.

14. (Original) The method of claim 12, wherein the step of automatically removing patient identifying information from an image comprises manually identifying burned-in patient identifying information within an image and automatically blanking the identified patient identifying information.

15. (Original) The method of claim 1, further comprising the steps of:

      mapping the encrypted ID to a Study ID that comprises an arbitrary human readable ID which contains no patient identifying information; and

      generating a data structure that includes the mapping.

16. (Original) The method of claim 15, further comprising mapping the Study ID to one or more replacement strings that can be used to replace de-identified data in the de-identified data record.

17. (Original) The method of claim 15, further comprising making the data structure publicly accessible.

18. (Original) The method of claim 15, further comprising using the encrypted ID or corresponding Study ID to recognize a subject patient of patient data records collected at different times.

19. (Original) The method of claim 1, wherein the method is implemented for sharing patient data for purposes of research.

20. (Original) The method of claim 1, wherein the method is implemented for sharing patient data for purposes of central monitoring for natural or human induced disease outbreaks.

21. (Currently Amended) A program storage device readable by a machine, tangibly embodying a program of instructions executable on the machine to perform method steps for processing medical information, the method steps comprising:

      obtaining a patient data record of a patient which includes patient identifying information;

removing the patient identifying information from the patient data record to generate a de-identified data record comprising unencrypted patient data in the patient data record which does not identify the patient;

generating an encrypted ID for the patient, wherein the encrypted ID comprises an encrypted representation of one or more items of patient identifying information; and

storing the encrypted ID with or in the de-identified data record,

wherein the instructions for removing the patient identifying information in the patient data record comprise instructions for automatically removing patient identifying information from an unstructured data record by locating a text string in the unstructured data records that includes patient identifying information and removing the text string from the unstructured data record, wherein the text string to be removed from the unstructured data record is determined based on a matching text string that is included in a database element of a structured data record associated with the unstructured data record.

22. (Original) The program storage device of claim 21, wherein the instructions for generating an encrypted ID for the patient comprise instructions for encrypting the one or more items of patient identifying information using a public key.

23. (Original) The program storage device of claim 21, further comprising instructions for securely maintaining a decryption key, which can be accessed by an authorized entity to decrypt the encrypted ID in the de-identified data record to re-identify the patient.

24. (Original) The program storage device of claim 23, wherein the decryption key is a private key that is associated with the public key for encryption.

25. (Original) The program storage device of claim 23, wherein the decryption key is a master private key that can decrypt de-identified data produced from many encryption/decryption key pairs.

26. (Original) The program storage device of claim 21, wherein the instructions for removing the patient identifying information in the patient data record to generate a de-identified data record is performed in compliance with a Safe Harbor rule or Limited Data set Rule of HIPAA.

27. (Original) The program storage device of claim 21, wherein the step of removing the patient identifying information in the patient data record includes automatically removing patient identifying information from a structured data record.

28. (Original) The program storage device of claim 27, wherein the instructions for automatically removing patient identifying information from a structured data record comprise instructions for removing database elements that contain patient identifying information.

29-31. (Canceled)

32. (Original) The program storage device of claim 21 wherein the instructions for removing the patient identifying information in the patient data record comprise instructions for automatically removing patient identifying information from an image.

33. (Original) The program storage device of claim 32, wherein the instructions for automatically removing patient identifying information from an image comprise instructions for removing patient identifying information contained in structured fields.

34. (Original) The program storage device of claim 21, further comprising instructions for performing the steps of: mapping the encrypted ID to a Study ID that comprises an arbitrary human readable ID which contains no patient identifying information; and generating a data structure that includes the mapping.

35. (Original) The program storage device of claim 34, further comprising instructions for mapping the Study ID to one or more replacement strings that can be used to replace de-identified data in the de-identified data record.

36. (Currently Amended) A method for processing data, comprising the steps of:

obtaining a data record of an individual which includes individual identifying information;

removing the individual identifying information from the data record to generate a de-identified data record comprising unencrypted data in the data record which does not identify the individual;

generating an encrypted ID for the individual, wherein the encrypted ID comprises an encrypted representation of one or more items of individual identifying information; and

storing the encrypted ID with or in the de-identified data record,

wherein the step of removing the individual identifying information from the data record includes automatically removing the individual identifying information from an unstructured data record by locating a text string in the unstructured data records that includes the individual identifying information, and removing the text string from the unstructured data record, wherein the text string to be removed from the unstructured data record is determined based on a matching text string that is included in a database element of a structured data record associated with the unstructured data record.

37. (Original) The method of claim 36, wherein the data record comprises medical information.

38. (Original) The method of claim 36, wherein the data record comprises financial information.

39. (Original) The method of claim 36, further comprising securely maintaining a decryption key, which can be accessed by an authorized entity to decrypt the encrypted ID in the de-identified data record to re-identify the individual.

40. (Previously Presented) A system for processing data, comprising:

a first data processing system comprising:

a first repository that stores data records of an individual which include individual identifying information; and

an encryption system that can generate an encrypted ID for the individual using an encryption key associated with the first data processing system, wherein the encrypted ID comprises an encrypted representation of one or more items of individual identifying information, and wherein the encryption system can generate de-identified data records of the individual which are associated with the encrypted ID, wherein the de-identified data records of the individual comprise unencrypted data in the data records which does not identify the individual; and

a second data processing system comprising:

a second repository that stores de-identified data records generated by the first data processing system; and

an engine that processes the de-identified data records in the second repository; and

a third data processing system comprising:

a third repository that stores a master decryption key; and

an encryption system that can use the master decryption key to decrypt an encrypted ID of de-identified data records in the second repository to re-identify the individual.

41. (Original) The system of claim 40, wherein the third data processing system is operated by an entity that is authorized or legally empowered to re-identify de-identified data records.